PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-143621
(43)Date of publication of application : 29.05.1998

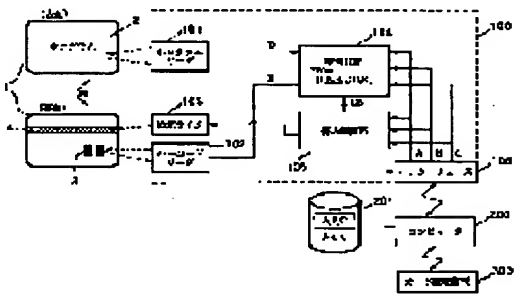
(51)Int.CI. G06K 17/00
G03H 1/22
G06F 17/60
G06F 19/00
G06K 19/10
G06K 19/06

(21)Application number : 08-286490
(22)Date of filing : 29.10.1996

(71)Applicant : AMERICAN BANK NOTE HOLOGRAPHIC INC
(72)Inventor : LILLEY OBOIIRU
DAA KUAN KAN

(54) CARD SECURITY SYSTEM, METHOD FOR IMPROVING SECURITY, CARD READING DEVICE AND CARD ISSUING DEVICE AND HOLOGRAM READING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To efficiently improve security in a card security system using an identification card or the like.
SOLUTION: In a card security system equipped with a card issuing device 100 and a card reading device 300, the card issuing device 100 reads a hologram 2 and a bar code 3 on a card 1, and obtains data D and E. Also, data A, B, and C are inputted from a computer 200 to the card issuing device 100. An enciphering part 104 generates check data EN based on the data A-E, and a magnetic writer 103 writes the data A-C and EN in a magnetic stripe 4. The card reading device 300 reads the data A-E from the card 1, calculates check data by using this, and compares the check data with the check data EN recorded in the magnetic strip 4 for judging the authenticity of the card.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－143621

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00		Ｔ
Ｇ０３Ｈ　1/22		Ｇ０３Ｈ　1/22		
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21		３４０Ｃ
19/00		15/30		３５０Ｚ
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00		Ｒ

審査請求　未請求　請求項の数21　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平8－286490

(22)出願日　平成８年(1996)10月29日

(71)出願人　594074779
アメリカン　バンク　ノート　ホログラフィクス，インク．
アメリカ合衆国　10523　ニューヨーク、エルムスフォード　イグゼキュティブ　ブルバード　399

(72)発明者　リリィ　オボイール
アメリカ合衆国　ニューヨーク州　コートランド　マナー　（番地無し）

(72)発明者　ダー・クアン　カン
アメリカ合衆国　ニューヨーク州　クロートン　オン　ハドソン　（番地無し）

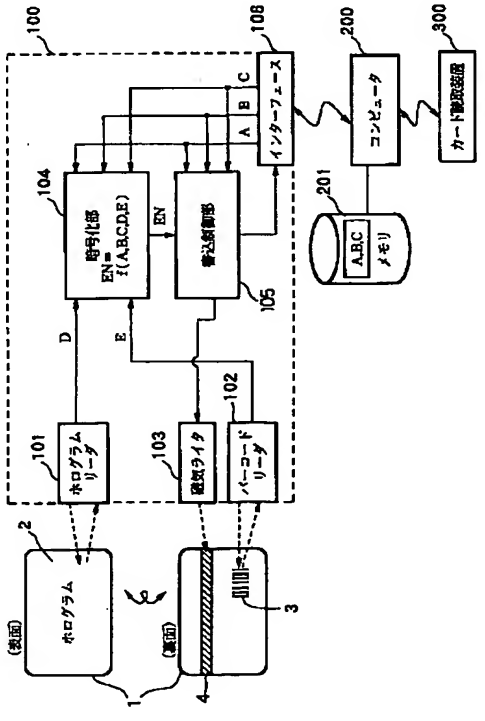
(74)代理人　弁理士　大塚　康徳　（外１名）

(54)【発明の名称】　カードセキュリティシステム及びセキュリティ向上方法及びカード読取装置及びカード発行装置及びホログラム読取装置

(57)【要約】

【課題】識別カード等を用いたカードセキュリティシステムにおけるセキュリティを効果的に向上する。

【解決手段】カード発行装置１００とカード読取装置３００を備えるカードセキュリティシステムにおいて、カード発行装置１００はカード１上のホログラム２及びバーコード３を読み取りデータＤ、Ｅを得る。また、コンピュータ２００よりカード発行装置１００にデータＡ、Ｂ、Ｃが入力される。暗号化部１０４は、データＡ～Ｅに基づいてチェックデータＥＮを生成し、磁気ライタ１０３はデータＡ～Ｃ及びＥＮを磁気ストライプ４に書込む。カード読取装置３００では、カード１よりデータＡ～Ｅを読み取り、これらを用いてチェックデータを算出し、磁気ストライプ４に記録されたチェックデータＥＮと比較することでカードの真正を判断する。



【特許請求の範囲】

【請求項１】　カード発行装置とカード読取装置を備えるカードセキュリティシステムにおけるセキュリティの向上方法であって、
カード上の光学的読取部分に少なくとも第１のデータを記録する第１記録工程と、
前記カード発行装置に少なくとも第２のデータを入力する入力工程と、
少なくとも前記第１のデータと前記第２のデータに基づいてチェックデータを獲得する獲得工程と、
少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する第２記録工程と、
少なくとも前記光学的読取部分を読み取って得られるデータと、前記格納媒体より得られるデータと、前記入力工程で用いられた前記第２のデータとに基づいて、前記カード読取装置によりカードの正当性を検証する検証工程とを備えることを特徴とするセキュリティの向上方法。

【請求項２】　前記格納媒体は、前記カード上の磁気的読取部分あるいは光学的読取部分、前記カードに搭載されたメモリ、あるいは該カードとは別体のメモリの少なくとも１つで構成されることを特徴とする請求項１に記載のセキュリティの向上方法。

【請求項３】　前記第２記録工程は、前記チェックデータ及び前記第２のデータを前記格納媒体に記録し、
前記検証工程は、前記チェックデータ及び前記第２のデータとしてのデータを前記格納媒体より得ることを特徴とする請求項１に記載のセキュリティの向上方法。

【請求項４】　前記格納媒体は、前記カード上の磁気的読取部分及び前記カードとは別体のメモリを含み、
前記第２記録工程は、全チェックデータ及び前記第２のデータを前記磁気的読取部分と前記メモリに分けて記録することを特徴とする請求項３に記載のセキュリティの向上方法。

【請求項５】　前記第１記録工程は前記第１のデータをホログラフィックイメージにて記録することを特徴とする請求項１に記載のセキュリティの向上方法。

【請求項６】　前記獲得工程は、少なくとも前記第１のデータと前記第２のデータを暗号化することにより前記チェックデータを決定することを特徴とする請求項１に記載のセキュリティの向上方法。

【請求項７】　カード発行装置とカード読取装置を備えるカードセキュリティシステムであって、
カード上の光学的読取部分より少なくとも第１のデータを読み取る読取手段と、
前記カード発行装置に少なくとも第２のデータを入力する入力手段と、
少なくとも前記第１のデータと前記第２のデータに基づいてチェックデータを獲得する獲得手段と、
少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する記録手段と、
少なくとも前記光学的読取部分を読み取って得られる第１のデータと、前記格納媒体より得られるチェックデータと、前記入力手段で用いた前記第２のデータとに基づいて、前記カード読取装置によりカードの正当性を検証する検証手段とを備えることを特徴とするカードセキュリティシステム。

【請求項８】　光学的読取部分を含むカードの読み取りを行うためのカード読取装置であって、
少なくとも第１のデータを前記光学的読取部分より読み取る光学読取手段と、
少なくとも第２のデータ及び第３のデータを格納媒体より獲得する第１獲得手段と、
少なくとも前記第１のデータおよび前記第２のデータに基づいてチェックデータを算出する第２獲得手段と、
前記第１獲得手段で獲得した第３のデータと前記第２獲得手段で獲得したチェックデータとを比較し、当該カードが正当か否かを判定する判定手段とを備えることを特徴とするカード読取装置。

【請求項９】　前記格納媒体は、前記カード上に設けられた磁気的読取部分、光学的読取部分、該カードに搭載されたメモリ、あるいは該カードとは別体のメモリユニットの少なくとも１つによって構成されることを特徴とする請求項８に記載のカード読取装置。

【請求項１０】　前記第１獲得手段は、前記第２のデータを前記メモリユニットより獲得し、前記第３のデータを前記磁気的読取部分より獲得することを特徴とする請求項９に記載のカード読取装置。

【請求項１１】　前記格納媒体は前記カード上の磁気ストライプを含み、
当該カードの使用後に前記磁気ストライプ上のデータを無効化する無効化手段を更に備えることを特徴とする請求項８に記載のカード読取装置。

【請求項１２】　カードの発行を行うカード発行装置であって、
光学的読取部分より少なくとも第１のデータを読み取る読取手段と、
カードとは別体の記憶部より少なくとも第２のデータを入力する入力手段と、
少なくとも前記第１のデータおよび前記第２のデータに基づいてチェックデータを決定する決定手段と、
少なくとも前記決定されたチェックデータを格納媒体に記録する記録手段とを備えることを特徴とするカード発行装置。

【請求項１３】　前記格納媒体は、前記カード上に設けられた磁気的読取部分、光学的読取部分、該カードに搭載されたメモリあるいは該カードとは別体のメモリユニットの少なくとも１つによって構成されることを特徴と

する請求項１２に記載のカード発行装置。
【請求項１４】　前記記録手段は、前記チェックデータを当該カード上の磁気的読取部分に記録し、前記第２のデータを前記メモリユニットに記録することを特徴とする請求項１３に記載のカード発行装置。
【請求項１５】　ホログラムイメージ上に所定の方向から光を照射する照射手段と、
前記照射手段で照射された光の前記ホログラムイメージからの反射光によって空間に形成される再生像の光強度分布を検出する検出手段と、
前記検出手段で検出された光強度分布を出力する出力手段とを備えることを特徴とするホログラム読取装置。
【請求項１６】　前記再生像の相対的な光強度に基づいて前記検出手段によって検出された前記光強度分布を２値化する２値化手段を更に備え、
前記出力手段は前記２値化手段で得られる２値化データを出力することを特徴とする請求項１５に記載のホログラム読取装置。
【請求項１７】　異なるパターン像を形成するべく前記再生像を処理する処理手段を更に備え、
前記検出手段は、前記パターン像の光強度分布を検出することを特徴とする請求項１５に記載のホログラム読取装置。
【請求項１８】　前記処理手段は、所定のパターン像を前記再生像に干渉させることで該再生像を処理することを特徴とする請求項１７に記載のホログラム読取装置。
【請求項１９】　前記検出手段で検出された光強度分布に対応するパターンデータをディジタル的に処理し、別のパターンデータを形成する処理手段を更に備え、
前記出力手段は前記処理手段で形成された前記別のパターンを出力することを特徴とする請求項１５に記載のホログラム読取装置。
【請求項２０】　ホログラムイメージ上に所定の方向から光を照射する照射手段と、
前記照射手段で照射された光の前記ホログラムイメージからの反射光に所定の光波を干渉させ、パターンイメージを形成する干渉手段と、
前記干渉手段で形成されたパターンイメージの光強度分布を検出する検出手段と、
前記検出手段で検出された光強度分布を出力する出力手段とを備えることを特徴とするホログラム読取装置。
【請求項２１】　前記ホログラムイメージはフーリエ変換パターンであることを特徴とする請求項１５乃至２０のいずれかに記載のホログラム読取装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、クレジットカード、ＩＤカード、運転免許証等の如き識別カードを利用したカードセキュリティシステム及びセキュリティ向上方法及びカード読取装置及びカード発行装置及び該カードセキュリティシステムに好適なホログラム読取装置に関する。
【０００２】
【従来の技術】クレジットカードが発行された初期の時代は、銀行がカードを見境なく発行し、ブランクカードに対する管理は手ぬるかった。すなわち、多くのカードに銀行名を入れただけのブランクのクレジットカードが存在し、これらが犯罪者に利用されていた。さらに、カードの信頼性を保つための印刷手法も欠如していたので、犯罪者は容易に真正カードに代わる偽造カードをつくることができ、このような犯罪が多発していた。
【０００３】銀行側の損失がエスカレートするにつれて、銀行はカードの発行を許可する顧客を厳しく制限するとともに、カード自体のデザインや製造上のセキュリティを向上する手段を講ずるようになった。多くの手段が考えられが、犯罪者にとっての主たるカード資源、すなわち、偽造カードを事実上なくしたのは、ホログラフィーによって生成した回折格子を有する一枚の箔をカードの前面に導入することであった。しかし、それでも犯罪者には、次の３つの理由に基づく詐欺行為の道が残されていたのである。
【０００４】第１は、盗難もしくは遺失カードで、カード所有者からの報告が届くまでの間に、これを使用することである。第２は、旧式もしくは遺失カードではあるが、かつて有効なカードであったものに有効な口座番号を再コード化して使用することである。第３は有効番号を使用する（カード無しに）こと、もしくはＡＴＭで使用するための磁気ストライプを有する白カードを使用すること、或いは、人による認証ではなく機械読みのみによる認証が行われる電話を使用することである。実際には、カード自体が正当なものであると断言しようとする第４のタイプの詐欺行為もある。マスターカードとビザがこの分野においてホログラムを８年間用いてきた。しかし、間もなく、何者かが、何処かで、受容され得る偽造カードを製造するのに十分な技術を獲得するようになるであろう。よって、犯罪者の偽造行為に一歩先んじた防衛手段のための安全印刷の時機が再び到来したと考えるべきである。
【０００５】
【発明が解決しようとする課題】今日の技術では第１の盗難もしくは遺失タイプの詐欺行為については防衛手段は殆どない。しかしながら、本発明は、第２、第３、第４のタイプの犯罪行為に対しては安全性を有効に増進することができる。
【０００６】典型的なクレジットカード取引は販売員がカードを見て、有効と思えば、カードを磁気リーダに打ち込む。これは Chang et alの米国特許第 4,788,420号に開示された方法である。リーダは取引口座アクセス識別番号を認証元に送り戻す。そして、認証元から許諾の応答があれば取引が実行される。結局、合法的なカード

の所有者が計算書を受け取り、当該所有者はこの計算書に対して支払いもしくは否認をすることになる。もし、カードの所有者によって正当に否認されると、磁気リーダは手続上認可された取引口座アクセス識別番号を提供したのであるから、結局は銀行が損失を吸収しなければならないであろう。これが第１及び第２のタイプの詐欺において発生するのである。

【０００７】磁気ストライプに書き込まれたりコード化された取引口座アクセス識別番号は車のナンバープレートに非常によく似ている。ナンバープレートには沢山の情報はないし、磁気ストライプにも沢山の情報がない。支払いの歴史、顧客の母親の旧姓等、真に価値ある情報は、すべて銀行の情報システムの奥に貯蔵される。そのクレジットが有効かどうかのみが、販売現場からの要求によって到達する。

【０００８】上記の状況は自動車のプレートないしは登録ナンバーに似ている。すなわち、情報はあまり沢山ではなく、丁度、自動車省のファイルに貯蔵されている情報に到達する手法である。

【０００９】顧客側の少量の銀行情報（カードの有効期間、有効なクレジット量）へのアクセスは、取引を読み取り報告するのに利用できる装置によってクレジットカードが打ち込まれ或いは磁気的に読み取られた際に、電子ネットワークを介して随時商人に利用可能である。

【００１０】不法な目的のための一般に受容され得るクレジットカードの供給は不完全かつ少量であるが、物理的には真正であるが旧式になってしまったクレジットカードを取得して磁気情報を変えたり、カード上面の満了期日や氏名を再エンボス加工することは、犯罪者には依然として比較的容易である。元の氏名を消して再エンボスしたものは完全ではないのにもかかわらず、このような詐欺に慣れた人の周到な準備によって、この世俗的な詐欺手段は一般には成功する。そこで、カードを打って、クレジット相当の勘定が識別され、マシンには取引有効の緑信号が出る。

【００１１】とくにＡＴＭのような場合では、犯罪者が唯一必要とすることは、磁気的に読み取れる取引口座アクセス識別番号と、何も知らない被害者の個人識別番号（ＰＩＮ）とをコード化した磁気テープを有する白カードである。また、電話室とか、スーパーマーケットのような、個人識別番号が不要であり、事務員による実カードの照合がなされないような場所も沢山ある。

【００１２】磁気エンコードのセキュリティを高めたり、書換を妨げるような試みが長期に亘って積極的に試みられた。 Thorne-EMI の Watermark（商標）テープがその一例であった。３M社等の高エルステッドテープの開発も同じ例である。両者とも、幾らか限定されたものではあるが、セキュリティの向上をそれぞれの方式において提供した。しかし、両者とも、現在使われている処理を変更しなければならないため、業界には受容されなかった。

【００１３】Thorne-EMIの方法はテープが製造されている間にテープに連続番号を磁気的に組み込んでしまうという方法である。これは磁気リーダで読み取りができる。しかし、この方法はテープ製造の困難さや、連続番号であることもあって挫折した。このような方法はコストが掛かり過ぎると考えられている。

【００１４】３M社の方法は３００エルステッドテープ（業界の規準）をコード化するのに使用されるものよりも、もっと強力なコード化装置が必要な高い飽和保磁力を有するテープの製造ということであった。このような装置は容易には得られないので、安全性が辛うじて増進された。業界はさらに強い飽和保磁力テープを指向した。しかしサービス業も銀行もこれにあわせて新しいエンコード装置を買い求めなければならなかった。これは、そうすることに確固たる動機を持ち合わせないグループにとっては大きな設備投資であり、このような高い飽和保磁力テープのエンコード装置が犯罪者には利用されないのであるという見通しもなかった。以上のような状態で、強力なテープも装置も、僅かな変化しか期待することができなかった。

【００１５】磁気的な読取環境に記録されたものはどんなものであっても、磁気エンコードを読み取る初歩的な装置によって誰でも読み取ることができる。コード化され、或いは暗号化されることによって数字が意味をなさなくとも、そのコード化された、或いは暗号化された数字を模写することは依然として容易である。過去に欠如していたものは、即ち本発明が解決しようとするものであるが、従来の装置では読み取ることのできないもう一つのレベルの、費用効果の良い方法で磁気ストライプに書込みが可能な数字である。

【００１６】磁気番号のアルゴリズムを含むすべての他のいかなる努力も、それがどんなに入り組んだ複雑なものであっても弱点を有している。その理由は、オリジナルであっても偽造したものであっても、全ての磁気番号を磁気リーダで読み取ることができ、読み取った番号を検証のために、通信網に乗せて銀行に送ることができるからである。

【００１７】問題解決の方法として、カード製造会社が大部分のクレジットカードにバッチナンバーを印刷している。全てのアメリカンエキスプレスのカードや幾つかのマスターカードに見られる４桁数字が一般的である。取引が詐欺らしいという疑いがある時は、カードの有効性について発行銀行に電話をして、ａ）バッチ番号は真正であって盗用されたものではないか、ｂ）カードの上の個人に係属する磁気情報がカードの前面のバッチ番号に合致するかどうか、を調べるのである。

【００１８】この方法は、カードを差し出した相手が取引に相応しくない風体であった場合、例えば汚いスニーカーを履いた十代の若者が真新しい自動車を買おうとす

る場合とか、なにか落ち着かない状況にある場合にのみ詐欺だと決める不完全かつ努力を必要とする方法である。

【００１９】１９８９年８月８日発行の Tominyama et alの米国特許第 4,855,584号には別の方法が開示されている。これはカードを機械で２回読みすることで、データを電話連絡する必要をなくすものである。しかしながら、この方法では実際には磁気ストライプのように作用するバーコードを使うことによって証明媒体を隠してしまう必要がある。この実施できそうもないのみならず、磁気リーダにバーコード（磁気インクで印刷されている）を読ませ、そしてそのバーコードがＩＲリーダでのみ見られるように印刷されてあったとしても、詐欺師は下にある情報を、それが磁気的読取媒体であるため解読できる。

【００２０】全ての犯罪者が必要とすることは番号全体をコピーすることである。問題は、カラーゼロックス機でコピーすることができない視覚安全形態或いはシステムを創造しようとする試みに似ている。人間の視力が安全の形態を見ることができる限りはカラーコピー機もそれができる。すべての試みはコピー機を打ち負かすためになされてきたが、これを書いている時点ではすべての（極端に厄介な又は非実用的な）ものは失敗した。クレジットカードの確認という問題は、新規性があり非常に実際的な解決である。

【００２１】本発明は上述した問題に鑑みてなされたものであり、カード等のセキュリティを効果的に向上するカードセキュリティシステム及びそのセキュリティ向上方法及び該システムにおけるカード読取装置及びカード発行装置及び該カード読取装置に適用可能なホログラム読取装置を提供することを目的とする。

【００２２】

【課題を解決するための手段】上記の目的を達成するための本発明のカードセキュリティシステムにおけるセキュリティ向上方法は以下の工程を備える。すなわち、カード発行装置とカード読取装置を備えるカードセキュリティシステムにおけるセキュリティの向上方法であって、カード上の光学的読取部分に少なくとも第１のデータを記録する第１記録工程と、前記カード発行装置に少なくとも第２のデータを入力する入力工程と、少なくとも前記第１のデータと前記第２のデータに基づいてチェックデータを獲得する獲得工程と、少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する第２記録工程と、少なくとも前記光学的読取部分を読み取って得られるデータと、前記格納媒体より得られるデータと、前記入力工程で用いられた前記第２のデータとに基づいて前記カード読取装置によりカードの正当性を検証する検証工程とを備える。

【００２３】また、上記の目的を達成するための本発明のカードセキュリティシステムは以下の構成を備える。すなわち、カード発行装置とカード読取装置を備えるカードセキュリティシステムであって、カード上の光学的読取部分より少なくとも第１のデータを読み取る読取手段と、前記カード発行装置に少なくとも第２のデータを入力する入力手段と、少なくとも前記第１のデータと前記第２のデータに基づいてチェックデータを獲得する獲得手段と、少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する記録手段と、少なくとも前記光学的読取部分を読み取って得られる第１のデータと、前記格納媒体より得られるチェックデータと、前記入力手段で用いた前記第２のデータとに基づいて、前記カード読取装置によりカードの正当性を検証する検証手段とを備える。

【００２４】また、上記の目的を達成するための本発明のカード読取装置は、光学的読取部分を含むカードの読み取りを行うためのカード読取装置であって、少なくとも第１のデータを前記光学的読取部分より読み取る光学読取手段と、少なくとも第２のデータ及び第３のデータを格納媒体より獲得する第１獲得手段と、少なくとも前記第１のデータおよび前記第２のデータに基づいてチェックデータを算出する第２獲得手段と、前記第１獲得手段で獲得した第３のデータと前記第２獲得手段で獲得したチェックデータとを比較し、当該カードが正当か否かを判定する判定手段とを備える。

【００２５】また、上記目的を達成するための本発明のカード発行装置は以下の構成を備える。すなわち、、カードの発行を行うカード発行装置であって、光学的読取部分より少なくとも第１のデータを読み取る読取手段と、カードとは別体の記憶部より少なくとも第２のデータを入力する入力手段と、少なくとも前記第１のデータおよび前記第２のデータに基づいてチェックデータを決定する決定手段と、少なくとも前記決定されたチェックデータを格納媒体に記録する記録手段とを備える。

【００２６】更に、上記の目的を達成する本発明のホログラム読取装置は、ホログラムイメージ上に所定の方向から光を照射する照射手段と、前記照射手段で照射された光の前記ホログラムイメージからの反射光によって空間に形成される再生像の光強度分布を検出する検出手段と、前記検出手段で検出された光強度分布を出力する出力手段とを備える。

【００２７】更に、上記の目的を達成する本発明の他の構成によるホログラム読取装置は以下の構成を備える。すなわち、ホログラムイメージ上に所定の方向から光を照射する照射手段と、前記照射手段で照射された光の前記ホログラムイメージからの反射光に所定の光波を干渉させ、パターンイメージを形成する干渉手段と、前記干渉手段で形成されたパターンイメージの光強度分布を検出する検出手段と、前記検出手段で検出された光強度分布を出力する出力手段とを備える。

【００２８】なお、本発明において、カードとはいわゆるクレジットカードやＩＤカード等種々のカードを総称するものである。更に、本発明におけるカードは、銀行通帳のようなセキュリティを要する帳面、文書等をも含むものである。

【００２９】

【発明の実施の形態】以下、添付の図面を参照して本発明の好適な一実施形態を説明する。

【００３０】図１は、本実施形態のカードセキュリティシステムに用いられる識別カードの概観を示す図である。１は識別カードであり、その前面にはホログラムイメージ２が記録されている。そして、このホログラムイメージ２の全体あるいは一部分には、第１の光学的記録部分としてのホログラムコードが記録されている。また、識別カード１の裏面には、第２の光学的記録部分としてのバーコード３が印刷されている。更に識別カード１の裏面には、磁気ストライプ４が設けられている。なお、バーコード３としては、１次元バーコードが図示されているが、２次元バーコードを用いてもよい。

【００３１】図２は本実施形態のカードセキュリティシステムにおけるカード発行装置の構成を示すブロック図である。同図において、識別カード１は上述のごとく、その表面にはホログラムイメージ２を、裏面には磁気ストライプ４、バーコード３を有する。図１では、ホログラムイメージは識別カード１の表面の全体に記録されているが、カード表面の一部に記録されていてもよい。また、ホログラムコードの記録も、ホログラムイメージの一部もしくは全てとして記録される。ホログラムコードとしては、例えば３次元バーコードイメージが記録されており、後述のホログラムリーダ１０１によって読み取り可能である。

【００３２】１００は本実施形態のカード発行装置であり、カード発行装置１００は以下のように構成されている。１０１はホログラムリーダであり、識別カード１に記録されたホログラムに所定特性の光をあて、ホログラムイメージ２よりの反射光によって再生される再生像（３次元バーコードイメージ）から、当該ホログラムイメージ２に記録されているデータを読み取る。１０２は周知のバーコードリーダであり、本例では１次元バーコードであるバーコード３を読み取ってデータを得る。１０３は磁気ライタであり、磁気ストライプ４にデータを記録する。なお、ホログラムリーダ１０１が３次元バーコードイメージを走査して得た信号はディジタルデータに変換され、データＤとして出力される。また、バーコードリーダ１０２がバーコード３を走査して得た信号は、ディジタルデータに変換され、データＥとして出力される。

【００３３】１０４は暗号化部であり、ホログラムリーダ１０１がホログラムイメージ２を読み取って得たデータＤと、バーコードリーダ１０２がバーコード３を読み取って得たデータＥと、外部装置であるコンピュータ２００よりインターフェース１０６を介して得たデータＡ、Ｂ、Ｃを用いて所定の演算を行い、チェックデータＥＮを発生する（ＥＮ＝ｆ（Ａ、Ｂ、Ｃ、Ｄ、Ｅ）とする）。１０５は書込制御部であり、暗号化部１０４より得られたチェックデータＥＮを磁気ライタ１０３を介して磁気ストライプ４に書込む。更に、書込制御部１０５は、インターフェース１０６を介して入力されたデータＡ、Ｂ、Ｃを、磁気ライタ１０３を介して磁気ストライプ４に書込む。

【００３４】１０６はインターフェースであり、外部のコンピュータ２００と当該カード発行装置１００の間の通信を行う。コンピュータ２００はカード発行装置１００に接続されると共に、カード読取装置３００にも接続されており、この結果メモリ２０１はカード発行装置１００及びカード読取装置３００の何れからもアクセス可能である。なお、カード読取装置３００の詳細な構成については後述する。メモリ２０１にはデータＡ、Ｂ、Ｃが格納されており、カード発行装置１００からの要求を受けたコンピュータ２００がこれらのデータをカード発行装置１００に出力する。

【００３５】ここで、例えば、データＤとしては、当該カードの価値を示す金額データであり、データＥとしては当該カードの固有の番号を示す識別番号（ＩＤ）である。また、インターフェース１０６を介して入力されるコンピュータ２００よりのデータＡ、Ｂ、Ｃとしては、例えば、それぞれ日付、店番号、パスワードを示すデータである。以下の説明では、これらのデータが識別カード１に記録されるものとして説明する。

【００３６】なお、上述した磁気ストライプ４へ書込まれるデータＡ、Ｂ、Ｃ及びチェックデータＥＮの内の一部もしくはすべてをコンピュータ２００に接続されたメモリ２０１に格納しておくように構成することもできるが、この点は本実施形態の変形例において詳細に説明する。

【００３７】図３は本実施形態におけるカード読取装置の構成を示すブロック図である。ホログラムリーダ３０１は、処理対象である識別カード１に記録されたホログラムイメージ２上のホログラムコードを読み取り、これを当該カードの金額を示すデータＤｒとして暗号化部３０４へ出力する。バーコードリーダ３０２は、バーコード３を読み取り、これを当該カードの識別番号を示すデータＥｒとして暗号化部３０４へ出力する。磁気リーダ３０３は、磁気ストライプ４に記録されている、日付、店番号、パスワードを読み取り、データＡｒ、Ｂｒ、Ｃｒとして暗号化部３０４へ出力する。更に、磁気リーダ３０３は、磁気ストライプ４に記録されているチェックデータを読み取り、これをチェックデータＥＮｒとして判定部３０６へ出力する。

【００３８】３０４は暗号化部であり、入力されたデー

タＡｒ、Ｂｒ、Ｃｒ、Ｄｒ、Ｅｒに基づいてチェックデータＥＮｒ’を算出する。ここで、暗号化部３０４におけるチェックデータの算出アルゴリズム（暗号化演算）は暗号化部１０４（図２）のそれと同じである。３０５はインターフェースであり、コンピュータ２００とカード読取装置３００との間の通信を制御する。本実施形態のインターフェースは、ホログラムリーダ３０１、バーコードリーダ３０２、磁気リーダ３０３から得られるデータＡｒ～Ｅｒをコンピュータ２００に対して送信する。コンピュータ２００は、カード読取装置３００より受信したデータＡｒ、Ｂｒ、Ｃｒとメモリ２０１に格納されているデータＡ、Ｂ、Ｃとを比較して、データＡｒ、Ｂｒ、Ｃｒの正当性を検証する。そして、インターフェース３０５は、データの正当性を検証した結果をコンピュータ２００より受信する。この受信された正当性の検証結果は、判定部３０６へ入力される。

【００３９】なお、カード発行装置１００による識別カード１の発行時に、コンピュータ２００が発行対象の識別カードのＩＤ番号を入力し、ＩＤ番号とデータＡ、Ｂ、Ｃとを対応付けるテーブルをメモリ２０１に格納しておくようにしてもよい。この場合、カードの正当性の検証に際しては、カード読取装置３００より入力したＩＤ番号（データＥｒ）に基づいてテーブルを検索し、対応するデータＡ、Ｂ、Ｃを抽出する。そして、カード読取装置より入力したデータＡｒ、Ｂｒ、Ｃｒのそれぞれと比較することで、データの正当性をチェックするようにできる。こうすれば、Ａ、Ｂ、Ｃをカード毎に設定することができる。例えば、カード毎にパスワードを変更することが可能となる。

【００４０】判定部３０６は、磁気リーダ３０３が磁気ストライプ４より読み取ったチェックデータＥＮｒと、暗号化部３０４で得られたチェックデータＥＮｒ’とを比較する。判定部３０６は、この比較の結果両者が一致し、更にインターフェース３０５より入力された検証結果が正当であることを示している場合に、当該カードを受理し、処理部３０７に所定の処理の実行を指示する。本例では、読み取られた識別カード１のホログラムイメージ２として記録された金額データ（データＤｒ）に基づいて、現金の支払いを行うものとする。

【００４１】以上の構成を備えた本実施形態のカード発行装置１００、カード読取装置３００の動作をフローチャートを参照して説明する。

【００４２】図４は、第１の実施形態によるカード発行装置１００の動作手順を説明するフローチャートである。本例では、ホログラムコード（金額データ）を含むホログラムイメージとＩＤ番号を示す１次元バーコードとが記録されたカードをカード発行装置１００に供給しておき、磁気ストライプに所定のデータ書込が行われた識別カードが発行されるものとする。

【００４３】ステップＳ１１において、ホログラムリーダ１０１を用いて、供給された識別カード１のホログラムイメージ２を読み取り、データＤ（金額データ）を得る。また、ステップＳ１２において、バーコードリーダ１０２により識別カード１上のバーコード３を読み取り、データＥ（ＩＤ番号）を得る。更に、ステップＳ１３において、インターフェース１０６を介して外部コンピュータ２００よりデータＡ、Ｂ、Ｃ（日付、店番号、パスワード）を得る。

【００４４】続いて、ステップＳ１４において、暗号化部１０４が、データＡ～Ｅを用いて所定の演算処理（暗号化）を行い、チェックデータＥＮを発生する。ステップＳ１５では、書込制御部１０５の制御により、ステップＳ１３で獲得したデータＡ、Ｂ、Ｃと、ステップＳ１４で獲得したチェックデータＥＮとを磁気ライタ１０３によって磁気ストライプ４に書込む。以上のようにして磁気ストライプ４にデータが書込まれたカードは、当該カード発行装置のカード排出部（不図示）より、排出され、識別カードとして発行される（ステップＳ１６）。

【００４５】なお、本実施形態では、光学的記録部分（ホログラムコードとバーコード）が記録された状態のカードを供給してカードの発行を行うものとするが、ホログラムコードの記録、バーコードの印刷をカード発行装置において行うようにしてもよい。この場合、データＤ及びデータＥを発生し（或いはコンピュータ２００より入力し）、これに従ってホログラムコード、バーコードの記録を行うことになる。なお、この場合、データＤ、データＥは、記録に使用したデータを直接用いればよいので、カード発行装置１００のホログラムリーダ１０１、バーコードリーダ１０２は不要となる。

【００４６】図５は、本実施形態によるカード読取装置３００の動作手順を説明するフローチャートである。カード読取装置３００では、上述の手順で発行された識別カードの認証が行われる。

【００４７】まず、ステップＳ２１において、識別カード１のホログラムイメージに含まれるホログラムイメージ２をホログラムリーダ３０１で読み取り、これをデータＤｒ（金額データ）とする。また、ステップＳ２２において、識別カード１のバーコード３をバーコードリーダ３０２にて読み取り、これをデータＥｒ（ＩＤ番号）とする。更に、磁気リーダ３０３によって磁気ストライプ４を読み取り、データＡｒ、Ｂｒ、Ｃｒ（日付、店番号、パスワード）を得る。更にステップＳ２４では、磁気リーダ３０３が磁気ストライプ４よりチェックデータを読み取り、これをチェックデータＥＮｒとする。そして、ステップＳ２５において、暗号化部３０４が上記ステップＳ２１～２３で得られたデータＡｒ、Ｂｒ、Ｃｒ、Ｄｒ、Ｅｒを用いて所定の演算処理（暗号化）を行い、チェックデータＥＮｒ’を発生する。

【００４８】ステップＳ２６では、インターフェース３０５を介して、上記ステップＳ２１～Ｓ２３で獲得した

データＡｒ～Ｅｒをコンピュータ２００に送信し、コンピュータ２００によってこれらのデータの正当性の検証を行う。なお、コンピュータ２００による正当性の検証結果は、インターフェース３０５を介してカード読取装置３００に入力される。ここで、データの正当性の検証としては、例えば日付が期限切れを示しているとか、店番号やパスワードが一致しない等が挙げられる。更に、カード発行装置１００において読み取ったカードＩＤ番号（データＥ）をメモリ２０１に登録するように構成しておけば、カード番号の正、不正を判定することも可能である。もちろん、上述のように、カード毎にデータＡ、Ｂ、Ｃを異ならせる場合は、ＩＤ番号とデータＡ、Ｂ、Ｃを対応付けたテーブルを用いることになる。

【００４９】ステップＳ２７において、判定部3３０６は、コンピュータ２００からの検証結果をチェックし、これが不正を示していた場合は、ステップＳ３０において当該カードを拒否する。ここで、当該カードが不正である旨を表示するようにしてもよいことはいうまでもない。一方、コンピュータ２００からの検証結果が正当であることを示していれば、処理はステップＳ２７からＳ２８へ進む。ステップＳ２８では、磁気リーダ３０３で読み取ったチェックデータＥＮｒと、暗号化部３０４で算出したチェックデータＥＮｒ’とを比較し、両者が一致するか否かを調べる。両者が一致すれば、当該カードは正当であると判定され、ステップＳ２９にてホログラムイメージ２に記録されていた金額データ（データＤｒ）に従った金額が支払われる。一方、両者が一致しなければ、当該カードは不正であるとして、ステップＳ３０へ進み、当該カードを拒否する。

【００５０】なお、上記ステップＳ１１～ステップＳ１３、或いはステップＳ２１～Ｓ２４における各データの獲得は、これらフローチャートによって示された順番に限られるものではないし、実質的に同時に獲得されてもよい。

【００５１】また、上記実施形態では、カード読取装置３００がコンピュータ２００と通信することにより、データＡｒ、Ｂｒ、Ｃｒ等の正当性を検証するが、この構成は省略してもよい。即ち、図３に示したカード読取装置３００の構成のうちインターフェース３０５を省略し、図５のフローチャートからステップＳ２６、Ｓ２７を省略してもよい。この場合、磁気ストライプから得たチェックデータＥＮｒと暗号化部３０４で発生したチェックデータＥＮｒ’との一致を調べることのみで識別カードの正当性を判定することになるが、ホログラムコードとして記録されているデータＤによって、磁気ストライプ４に書込むべきチェックデータが変化するので、識別カードのセキュリティを効果的に向上することができる。

【００５２】なお、上記実施形態のカード読取装置において、使用済みとなったカードの磁気ストライプ４上に記録されたデータを消去あるいは無効化する構成を備えてもよい。

【００５３】次に、上記実施形態におけるセキュリティ向上システムの変形例を図６、図７を参照して説明する。

【００５４】図６は、本実施形態のセキュリティ向上システムにおける第１の変形例によるカード読取装置の構成を示す図である。なお、図６において図２と同じ構成には同一の参照番号を付し、ここでは説明を省略する。第１の変形例では、データＡ、Ｂ、Ｃを磁気ストライプ４に書き込まない。即ち、図４のステップＳ１５において、図２の書込制御装置１０５は磁気ライタ１０３を用いて暗号化部１０４より入力したチェックデータＥＮのみを磁気ストライプに書き込むことになる。

【００５５】さて、図６においてインターフェース３１０は、コンピュータ２００よりデータＡ、Ｂ、Ｃを受信し、これを暗号化部３０４へ出力する。暗号化部３０４は入力されたＡ、Ｂ、Ｃ、Ｄｒ、Ｅｒに基づいてチェックデータＥＮｒ’を生成する。そして、判定部３１１は、暗号化部３０４より得たチェックデータＥＮｒ’と磁気リーダ３０３が磁気ストライプ４を読み取って得たチェックデータＥＮｒとを比較し、両者が一致するか否かでカードの正当性を判定する。

【００５６】図７は第１の変形例におけるカード読取装置３５０の制御手順を示すフローチャートである。同図において、図５と同じ処理を行うステップには同一のステップ番号を付し、ここでは詳細な説明を省略する。ステップＳ４１では、インターフェース310を介して外部コンピュータ２００よりデータＡ、Ｂ、Ｃを獲得する。そして、ステップＳ４２では、獲得したデータＡ、Ｂ、Ｃ、Ｄｒ、Ｅｒに基づいて暗号化部３０４がチェックデータＥＮｒ’を算出する。そして、このチェックデータＥＮｒ’とステップＳ２４で獲得したチェックデータＥＮｒとを比較してカードの正当性が判定される。

【００５７】なお、上記第１の変形例では、磁気ストライプ４にチェックデータＥＮを記録し、データＡ、Ｂ、Ｃの記録は行わなかったが、データＡ～Ｃとチェックデータの保存先としては更に種々の変形が可能である。例えば、チェックデータＥＮとデータＡを磁気ストライプ４に記録するようにしてもよい。また、チェックデータＥＮの書込先をメモリ２０１としてもよい。以下、第２の変形例として、チェックデータＥＮの書込先をメモリ２０１とし、磁気ストライプ４には何も記録しない場合を説明する。

【００５８】図８は本実施形態のセキュリティ向上システムにおける第２の変形例によるカード読取装置の構成を示すブロック図である。第２の変形例では、図２のカード発行装置１００において、書込制御部１０５は、磁気ストライプ４へのチェックデータＥＮの書き込みを行わないほか、他のデータＡ～Ｃの書込みも行わないもの

とする。従って、識別カード１において磁気ストライプ４を省略することも可能である。そのかわりに、書込制御装置１０５は、コンピュータ２００に対してチェックデータＥＮ、データＤ（金額データ）、データＥ（ＩＤ番号）を送出するものとする。

【００５９】カード発行装置よりチェックデータＥＮ、データＤ、データＥを受け取ったコンピュータ２００は、データＤ、データＥにチェックデータＥＮを対応付けたチェックデータテーブル２０２（図８参照）を生成してメモリ２０１に記録する。なお、データＥが各識別カードに固有の番号を有するので、データＥのみを用いてチェックデータを登録するようにしてもよい。この場合、チェックデータテーブル２０２は、データＥとチェックデータＥＮのみを対応付けたテーブルとなる。要するに、カード読取装置３６０において識別カード１’のホログラムイメージ２もしくはバーコード３を読み取って得られたデータに基づいて、チェックデータテーブル２０２中のチェックデータを唯一特定できればよいのである。

【００６０】図８に示された識別カード１’には磁気ストライプが省略されており、カード読取装置３６０においては磁気リーダが省略されている。

【００６１】上述の第１の変形例と同様に、暗号化部３０４はインターフェース３２０を介してコンピュータ２００より入力したデータＡ、Ｂ、Ｃと、ホログラムリーダ３０１より入力したデータＤｒ及びバーコードリーダ３０２より入力したデータＥｒを用いてチェックデータＥＮｒ’を算出する。この算出されたチェックデータＥＮｒ’は判定部３１１へ入力される。

【００６２】一方、インタフェース３２０は、ホログラムリーダ３０１より得られたデータＤｒ及びバーコードリーダ３０２より得られたデータＥｒをコンピュータ２００へ出力する。コンピュータ２００は、カード読取装置３６０より入力されたデータＤｒ及びデータＥｒを用いてチェックデータテーブル２０２を検索し、対応するチェックデータＥＮを出力する。コンピュータ２００より出力されたチェックデータＥＮはインターフェース３２０を介して判定部３１１へ入力される。

【００６３】判定部３１１は暗号化部３０４より入力されたチェックデータＥＮｒ’とインターフェース３２０を介して入力されたチェックデータＥＮとを比較することにより当該識別カード１’の正当性を判定する。なお、第２の変形例におけるカード読取装置によるカードの正当性チェックの制御は、上述の図７とほぼ同様である。ただし、ステップＳ２４においてチェックデータＥＮ（図６のＥＮｒに相当する）を獲得するに際して、データＥｒ、データＤｒをコンピュータ２００に送り、その応答としてチェックデータＥＮを獲得する点が異なる。

【００６４】以上説明したように、上記実施形態のカードセキュリティ向上システムによれば、カード発行時において外部より与えられたデータＡ～Ｃ（実施形態ではコンピュータ２００より入力される）を用いてチェックデータの処理が行われる。従って、例えばデータＡ～Ｃを定期的に変更することでシステムのセキュリティを更に向上することが可能である。更に、チェックデータ算出のためにホログラムイメージ２が用いられるので、システムのセキュリティが向上する。

【００６５】なお、上記実施形態におけるデータの種類とその記録方法は一例にすぎず、種々の変更が可能であることはいうまでもない。たとえば、識別カードのＩＤ番号をホログラムコードとして登録するようにしてもよい。

【００６６】また、上記実施形態においてチェックデータ等を識別カード１に書き込む場合の書込先を磁気ストライプとしたが、ホログラムやバーコード等の光学的読取記録部分に記録するようにしてもよい。更に識別カードにＩＣメモリを搭載しておき、これに種々のデータを記録することも可能である。また、光学的読取部分や磁気的読取部分もカード上に複数個存在してよいことはいうまでもない。

【００６７】更に、上記実施形態では、コンピュータ２００をカード発行装置及びカード読取装置のいずれからも独立したものとしたが、コンピュータ２００はカード発行装置もしくはカード読取装置の何れか一方に内蔵されてもよい。また、この場合、カード発行装置、カード読取装置の何れかのＣＰＵがコンピュータ２００の機能を兼ね備えるものとしてもよい。

【００６８】また、上記実施形態のカードセキュリティシステムは、ホログラムイメージにホログラムイメージ２を含ませたことで、そのセキュリティをよりいっそう向上している。以下、本実施形態によるホログラムコードを記録したホログラムカードと、当該ホログラムコードを読みとるホログラムリーダの詳細な構成について説明する。

【００６９】ホログラムは、ホログラフィック手法あるいはダイレクトパターンイメージング手法を用いて記録される。ホログラムは、フーリエ変換型ホログラムであってもよいし、フレネル型ホログラムであってもよい。

【００７０】ここでは、フーリエ変換ホログラムを採用し、そのイメージパターンはバーコード像とする。更に、ホログラムのイメージパターンとしては、ランダムパターン、モアレパターン、逆フーリエ変換パターン等のいずれであってもよいし、これらの組み合わせであってもよい。図９はバーコード状パターンの一例を示す図である。以下では、このようなバーコード状パターンを再生するフーリエ変換パターンを記録する場合のホログラム記録と読取を説明する。

【００７１】図１０Ａ及び図１０Ｂは、フーリエ変換パターンのホログラム記録及び再生方法を説明する図であ

る。図１０Ａは典型的なホログラム記録の構成を示している。所定のパターン（本例では図９の如きバーコード状パターン）５１より距離ｆ（ｆはフーリエ変換レンズ５２の前方焦点距離）だけ離れた位置にフーリエ変換レンズ５２がセットされる。なお、パターン５１には、必要に応じて散光器が結合される。記録媒体５３は、フーリエ変換レンズ５２の後方に、当該レンズ５２の後方焦点距離（＝ｆ）だけ離れた位置に配置される。光源光５４をパターン５１に図示のように照射するとともに、参照光５５を記録媒体上へ所定角度θで照射する。すると、フーリエ変換レンズ５２を介して記録媒体５３へ到達するパターン光と参照光５４が記録媒体５３の面上で干渉し、パターン５１に対応するフーリエ変換ホログラムパターンが記録媒体５３の全体あるいは一部分に形成され、記録される。

【００７２】図１０Ｂには、フーリエ変換ホログラムにおける画像の再生方法が示されている。参照光５５の共役光としてのコリメート光５６を、当該ホログラムをエンコードした工程における参照光の照射角度θで、図示のように記録媒体５３に照射する。すると、フーリエ変換レンズ５７を介して、その前方焦点距離上に実像５８が再生される。なお、上記説明では、ホログラムの記録時にフーリエ変換レンズを用いたが、いわゆるレンズ無しフーリエ変換ホログラム記録の手法を用いることも可能である。

【００７３】上述のようなフーリエ変換記録手法は、高いセキュリティを提供する。なぜならば、ホログラム記録時の光学的仕様として、参照光の角度のみならず、その波長やフーリエ変換レンズの特性を知らない限り、当該ホログラムイメージを認識することが極めて困難だからである。

【００７４】図１１は、本実施形態によるカード読取装置のホログラムリーダの詳細な構成を説明する図である。

【００７５】７１は識別カード１上に形成されたホログラムイメージである。７２はホログラムを照射するための光源である。７３は、光源７２より照射された光によって再生された再生像である。なお、フーリエ変換ホログラムの場合は、ホログラムイメージ７１と再生像７３との間の適切な位置にフーリエ変換レンズ５７（図１０Ｂ参照）が配置されるが、図示を省略してある。ただし、ホログラムがいわゆるフレンネル型ホログラムであれば、そのような変換レンズは不要である。

【００７６】７４は光学的処理部であり、再生像７３を光学的に処理し、所定のパターン７５（本例ではバーコード状パターンであり、以下バーコードパターン７５という））を形成し、出力する。７６は光センサーであり、バーコードパターン７５を走査して、光強度に応じた信号を出力する。

【００７７】なお、本実施形態のホログラムリーダは、ホログラムイメージから最終的に図９のようなバーコード像を再生する。しかしながら、本実施形態のホログラムイメージは、当該バーコード像に所定のパターンを干渉させたイメージが記録されている。従って、フーリエ変換型ホログラム手法で記録されたホログラムイメージに適切な光源７２よりの光を照射することにより、不図示のフーリエ変換レンズを経て再生像７３が空間に検出され得るが、この再生像７３自体ではなんの意味もなさない。しかし、これが光学的処理部７４によって処理されると、バーコードパターン７５として空間に再生されるのである。

【００７８】図１２は光学的処理部７４の構成を示すブロック図である。同図において、再生像７３に対応する再生光はビームスプリッタ７４１を通過して、ミラー７４２で反射される。ミラー７４２による反射光はビームスプリッタ７４１で反射されて、９０度方向を換える。一方、干渉用入力パターンに対応する光がビームスプリッタ７４１を通過する。この結果、ミラー７４２で反射された再生光と干渉用入力パターン７４３に対応するパターン光とが干渉し、新たなパターン像が生成される。この新たなパターン像がバーコードパターン７５であり、読取可能なパターンとして光センサー７６に提供される。

【００７９】以上のように光学的処理部７４によって再生されたバーコードパターン７５は、光センサ７６によって検出される。光センサ７６は、バーコードパターン７５の光強度分布に応じた信号を信号処理部７９に出力する。信号処理部７９は、光センサ７６より入力された信号を２値データを示す矩形状のパルス列に変換する。ここで、２値化は、当該バーコードパターン７５の相対的な光強度分布に基づいてなされる。例えば、２値化のための閾値を、光センサの最大レベル（バーコードパターンの白部分）と最低レベル（バーコードパターンの黒部分）との値に基づいて決定する（たとえば両者の平均値）ようにすれば、より良好かつ確実にバーコードパターンを認識することができる。

【００８０】以上のように、ホログラムとして記録するパターンに、巧みに設計されたランダムパターンを用いれば、フーリエ変換面においてさえも、何の意味をも有していないパターンとしか認識されない。この場合、もう一つの別のパターンを用意しておき、再生されたランダムパターンを有意味なパターンに変換し、これを光センサ７６によって検出するようにする。ここで、ランダムパターンを有意味なパターンに変換するのが、光学的処理部７４である。そして、光センサ７６は、この有意味なパターンの光強度を検出し、信号処理部７９がこれの検出結果に基づいて２値データを発生する。たとえば、ホログラムイメージとしての記録にモアレパターンを用いた場合は、別のモアレパターンに干渉させることで、予め設計されたバーコードパターンを得ることがで

きる。

【００８１】なお、再生されたバーコードパターン７５の光センサ７６による走査は、光センサ７６がバーコードパターンを走査するような構成としてもよいし、光センサ７６は１点の光強度を検出し、読み取り時に識別カード１を移動させることによって再生像であるバーコードパターン７５を移動させ、この移動によってバーコードパターンを走査するようにしてもよい。

【００８２】また，再生像であるバーコードパターン７５の白黒パターンの強弱の度合は、カード表面の部分的な損傷や歪み等のためにオリジナルの記録イメージとは若干異なる可能性がある。しかしながら、光センサ７６及び信号処理部７９は、上述のごとく、光の相対的な強度を調べ、２値データとして出力するので、このような障害があってもバーコードパターンを正しく読み取ることができる。

【００８３】なお、光学的処理部７４は、ランダムパターンやモアレパターン、逆フーリエ変換パターンが記録されたホログラムコードを読み取る場合に必要な構成である。しかしながら、再生像がそのまま有意味なバーコードパターンとなる場合には、光学的処理部７４は不要である。図１３は光学的処理部を省略したホログラムリーダの構成を示す図である。光源７２よりの光をホログラムイメージ（ホログラムコード）に照射することで、空間にバーコードイメージ７７が再生されるので、光センサ７６によってその光の強度を直接的に読み取ることができる。なお、フーリエ変換形ホログラムの場合には、図１３の再生像７７とホログラム７１との間にフーリエ変換レンズが存在していることはいうまでもない。

【００８４】また、光学的処理部７４の機能をディジタル的に実現することも可能である。この場合、図１１の構成において、再生像７３の光強度分布を直接光センサ７６によって検出し、これをディジタルデータとして信号処理部７９に送る。信号処理部７９では、数値演算によって図１２の干渉用入力パターン７４３を干渉させたのと等価の処理を行う。この数値演算の結果得られる光強度分布のディジタルデータは、バーコードパターン７５に対応したものとなる。

【００８５】更に、光学的処理部７４は光波面の干渉を利用したものであってもよい。例えば球面波と平面波を干渉させると円形状の縞パターンが得られ、平面波と平面波を干渉させると、バーコード状の縞パターンが得られる。従って、例えば、ホログラムイメージからの再生光として球面波が得られるように構成し、光学的処理部７４において干渉用入力パターンとして平面波を入力すれば、バーコードパターン７５が得られるようになり、光センサで読み取ることができる。このようにホログラムからの反射光の位相分布によって情報を検出することも可能である。

【００８６】以上説明したように、上記実施形態によれば、特殊なデータチェックシステムを用いている上に、特殊なホログラムとホログラム検出方法を用いているのでカードセキュリティが飛躍的に向上する。更に再生されたホログラムパターンの認識を、パターンの相対的な光強度をチェックするということで行うので、カードの部分的な損傷等があっても、正しく認識を行うことができる。

【００８７】また、ホログラムイメージとして、他の所定パターンを干渉させることで初めて意味のある再生像を得られるよう構成したので、セキュリティがいちじるしく向上する。

【００８８】なお、上記信号処理部７９における２値データ（矩形信号）への変換は、バーコード等の技術において周知のセルフクロッキング（self-clocking）の方法に基づいて行われるものとする。また、識別カード表面の近くの空間へのイメージの再生は、一般の照明光では見ることができず、適した光学系（たとえば、ホログラムイメージへの光の照射角、照射光の波長、ホログラム記録時のフーリエ変換レンズに対応した適切な特性を有するフーリエ逆変換レンズ）によってのみ再生され、光センサ７６によって読み取ることが可能となる。このため、でセキュリティが向上する。

【００８９】

【発明の効果】以上説明したように、本発明によれば、カード等のセキュリティが効果的に、かつ飛躍的に向上する。

【００９０】

【図面の簡単な説明】

【図１】本実施形態のカードセキュリティシステムに用いられる識別カードの概観を示す図である。

【図２】本実施形態のカードセキュリティシステムにおけるカード発行装置の構成を示すブロック図である。

【図３】本実施形態におけるカード読取装置の構成を示すブロック図である。

【図４】第１の実施形態によるカード発行装置１００の動作手順を説明するフローチャートである。

【図５】本実施形態によるカード読取装置３００の動作手順を説明するフローチャートである。

【図６】本実施形態のセキュリティ向上システムにおける第１の変形例によるカード読取装置の構成を示す図である。

【図７】第１の変形例におけるカード読取装置３５０の制御手順を示すフローチャートである。

【図８】本実施形態のセキュリティ向上システムにおける第２の変形例によるカード読取装置の構成を示すブロック図である。

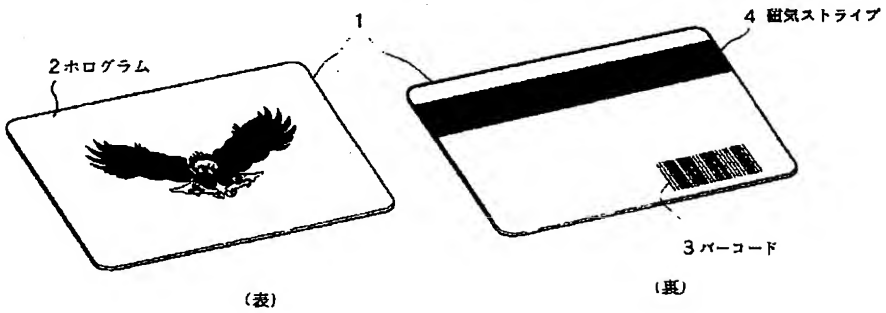
【図９】バーコード状パターンの一例を示す図である。

【図１０Ａ】フーリエ変換パターンのホログラム記録方法を説明する図である。

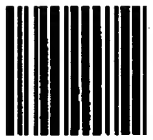
【図１０Ｂ】フーリエ変換パターンのホログラム再生方

法を説明する図である。
【図１１】本実施形態によるカード読取装置のホログラムリーダの詳細な構成を説明する図である。
【図１２】光学的処理部７４の構成を示すブロック図である。
【図１３】光学的処理部を省略したホログラムリーダの構成を示す図である。
【符号の簡単な説明】
１　識別カード
２　ホログラムイメージ
３　バーコード
４　磁気ストライプ
１００　カード発行装置
１０１　ホログラムリーダ
１０２　バーコードリーダ
１０３　磁気ライタ
１０４　暗号化部
１０５　書込制御部
１０６　インターフェース
２００　コンピュータ
２０１　メモリ
３００　カード読取装置

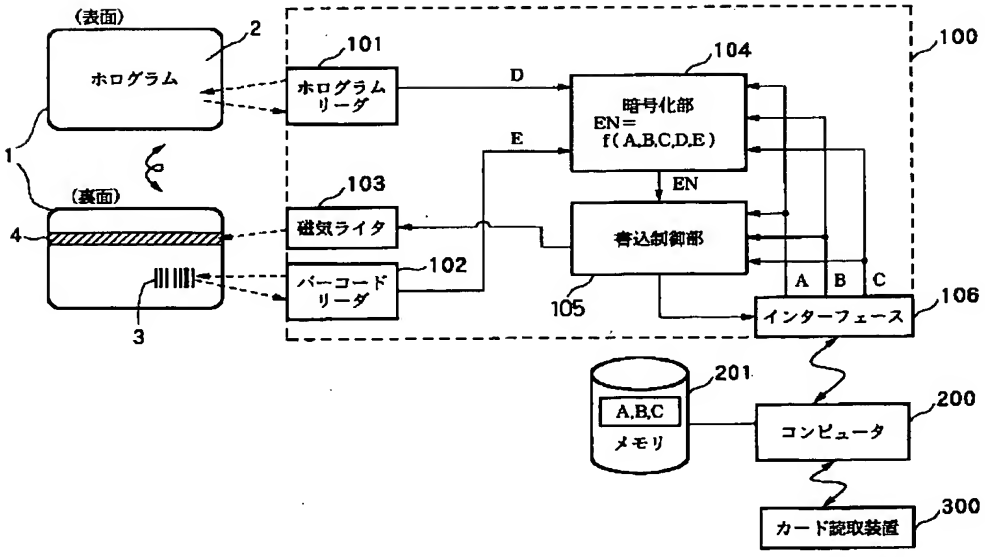
【図１】



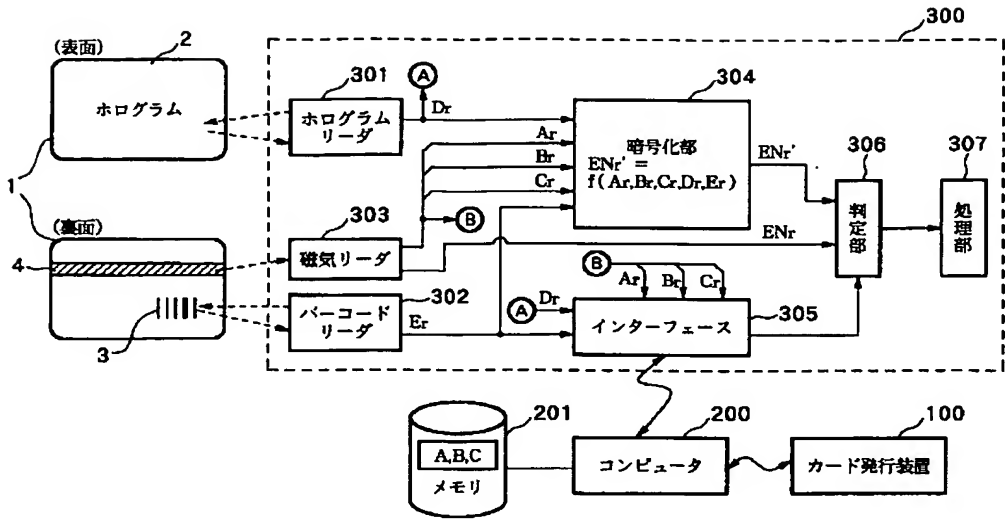
【図９】



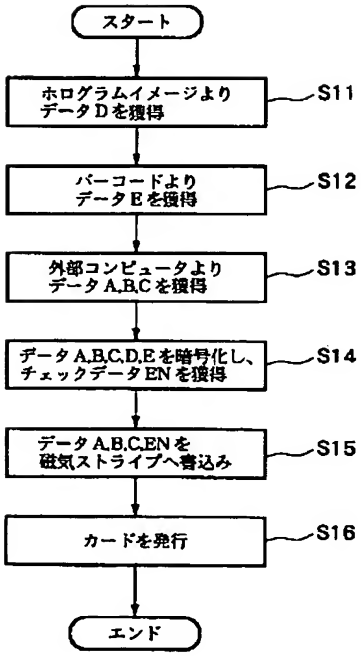
【図２】



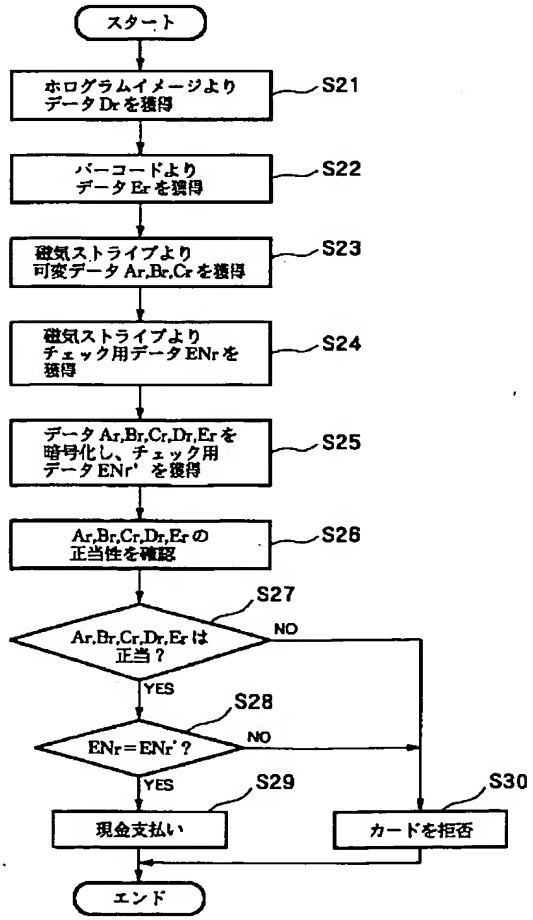
【図３】


300
(表面)
2
ホログラム
1
(裏面)
4
3
301
ホログラム
リーダ
303
磁気リーダ
302
バーコード
リーダ
A
Dr
Ar
Br
Cr
B
Er
304
暗号化部
ENr' =
f(Ar,Br,Cr,Dr,Er)
ENr'
ENr
306
判定部
307
処理部
Ar
Br
Cr
Dr
305
インターフェース
201
A,B,C
メモリ
200
コンピュータ
100
カード発行装置

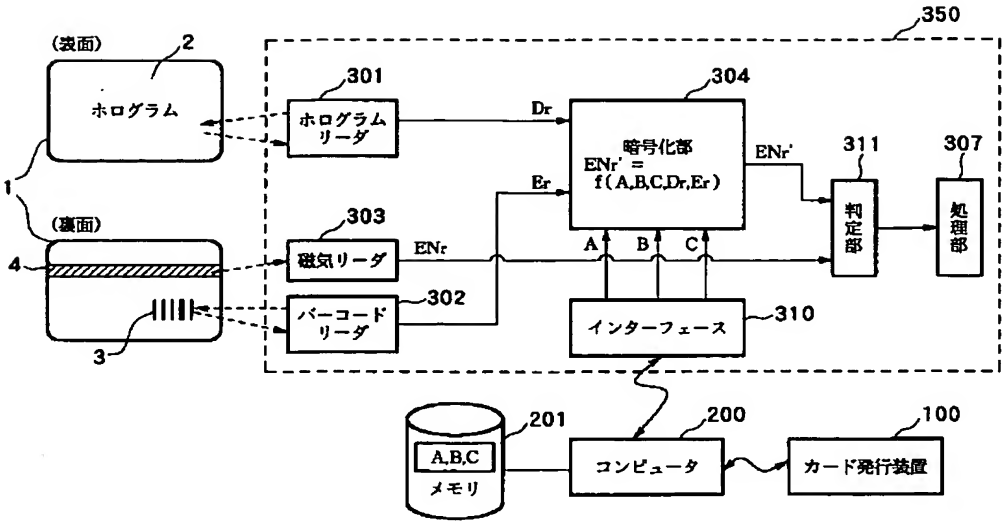
【図４】


スタート
ホログラムイメージより
データDを獲得
S11
バーコードより
データEを獲得
S12
外部コンピュータより
データA,B,Cを獲得
S13
データA,B,C,D,Eを暗号化し、
チェックデータENを獲得
S14
データA,B,C,EN を
磁気ストライプへ書込み
S15
カードを発行
S16
エンド

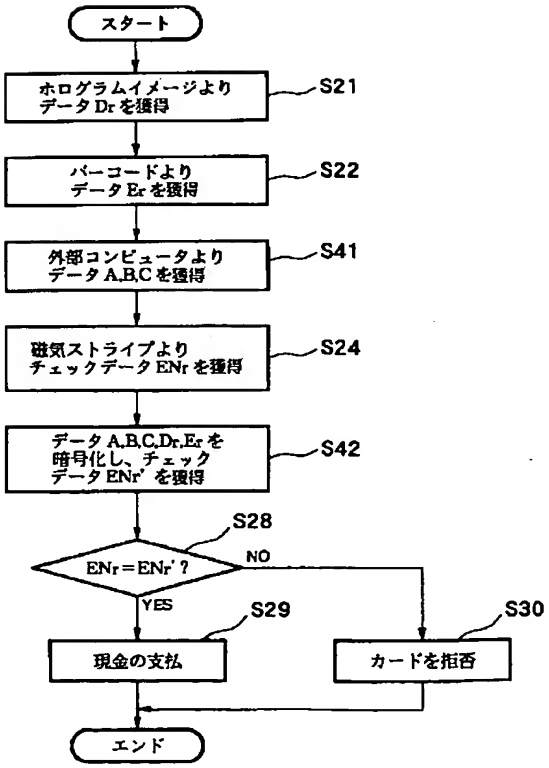
【図５】


スタート
ホログラムイメージより
データDrを獲得
S21
バーコードより
データErを獲得
S22
磁気ストライプより
可変データAr,Br,Crを獲得
S23
磁気ストライプより
チェック用データENrを
獲得
S24
データAr,Br,Cr,Dr,Erを
暗号化し、チェック用
データENr'を獲得
S25
Ar,Br,Cr,Dr,Erの
正当性を確認
S26
S27
Ar,Br,Cr,Dr,Erは
正当？
NO
YES
S28
ENr=ENr'？
NO
YES
S29
現金支払い
S30
カードを拒否
エンド

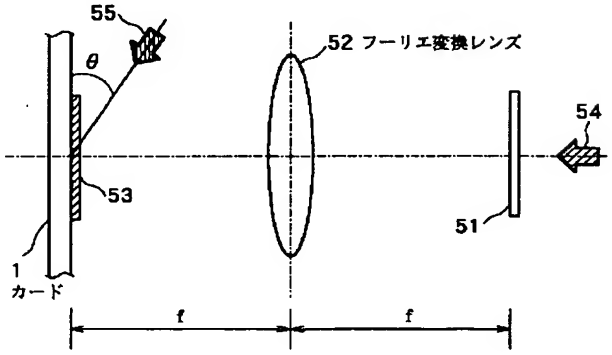
【図６】



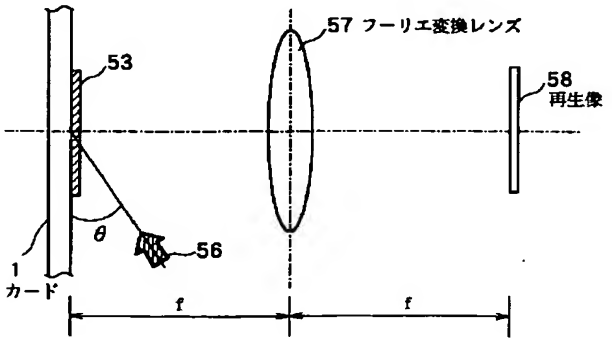
【図７】



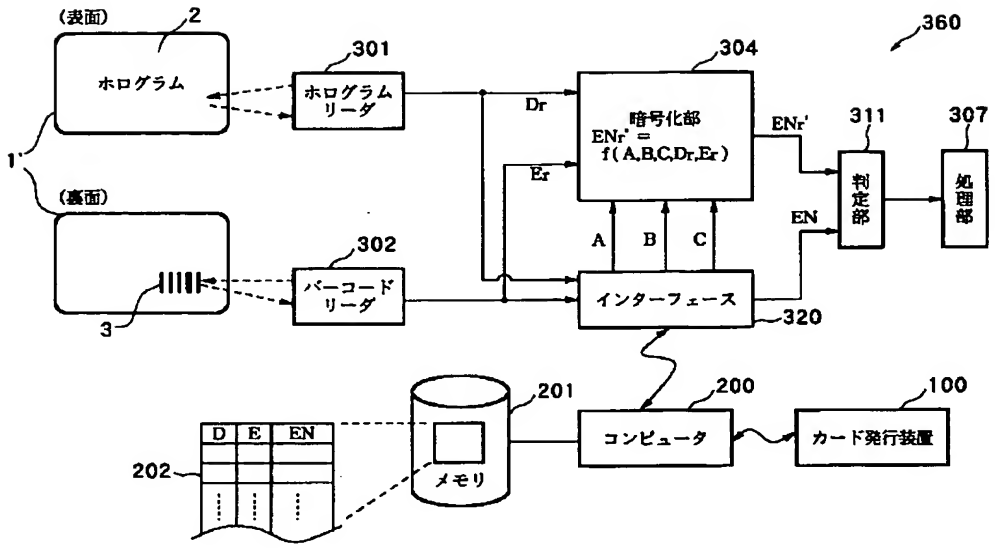
【図１０Ａ】



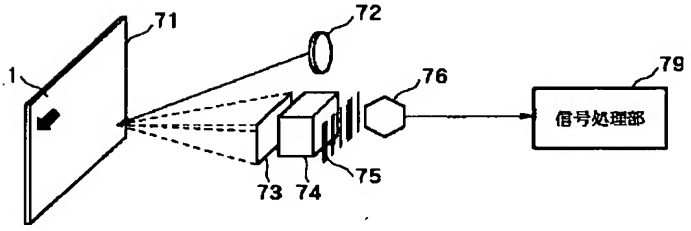
【図１０Ｂ】



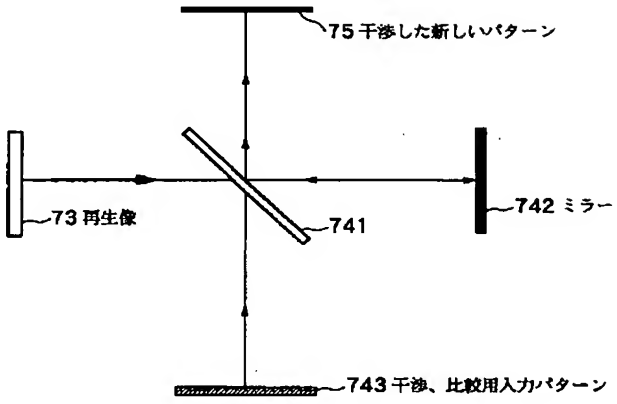
【図８】



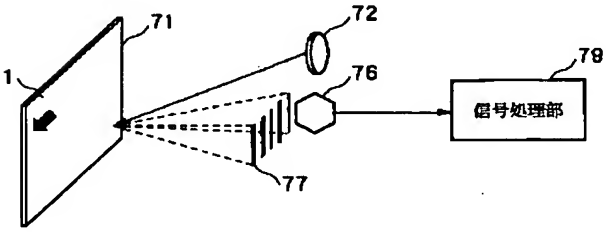
【図１１】



【図１２】



【図１３】



フロントページの続き

(51) Int.Cl.[6]	識別記号	FI	
G06K 19/06		G06K 19/00	D